Audit de sécurité

Abdelali Saidi

abdelali.saidi@gmail.com

Plan

Plan

Terminologie de la sécurité informatique

Menace

Une menace est l'indication de la possibilité de survenance d'un événement non désirable.

Vulnérabilité

Une vulnérabilité est l'existence d'une faiblesse qui peut amener à quelque chose d'inattendu.

Terminologie de la sécurité informatique

Attaque

Une attaque est un assaut sur un système informatique. L'attaque peut avoir l'un des deux aspects suivants:

- Passive
- Active

Exploit

L'exploit est le fait qu'une vulnérabilité soit exploitée par une attaque.

Types de pirates

- Black hats: les pirates qui utilisent leurs connaissances pour des objectifs malicieuse
- White hats: des pirates au même niveau que les black hats, qui teste les systèmes pour améliorer leur défense
- Grey hats: ce sont des pirates qui se situent entre les deux précédant types. Ils ont foi que le piratage est un art et non un acte de violence
- Hacktivists: ce terme fait référence aux groupes de personnes qui essayent de passer des messages (surtout politiques) par le biais d'Internet

L'objectif des pirates éthiques

Un pirate éthique essaye de répondre sur trois grandes questions:

- Que peut un pirate voir sur le système qu'il évalue?
- Que peut il faire sachant ce qu'il a vu?
- Est-ce que les tentatives du pirate seront remarquées sur le système?

Plan

Types de PenTests

Définition

Un test de pénétration est une simulation des méthodes qu'un pirate informatique utilise pour gagner un accès non autorisé au système informatique d'une entreprise. Elle peut être lancé sous forme:

- Boite noire: pour des tests sans aucune information à propos de l'organisation
- Boite grise: pour des tests avec des connaissances partielles de l'organisation
- Boite blanche: pour des tests avec une connaissance totale de l'organisation

Types de PenTests

Types de tests

- Réseau distant: le pirate éthique essaye de lancer une attaque depuis Internet
- Réseau local: ce test simule ce qu'un employé/sous-traitant/stagiaire peut corrompre.
- Vol d'équipement: le pirate éthique essaye de voir ce qu'il peut faire s'il utilise l'ordinateur d'un employé
- L'ingénierie sociale: mettre la crédulité des employés au test
- Effraction physique: essayer de s'infiltrer dans l'organisation

Les phases du PenTest

Présentation

Un test de pénétration suit en général trois phases:

- La reconnaissance
- Le Scanning
- Le gain de privilèges
- Maintenir l'accès
- Effacer les traces

Les phases du PenTest

La reconnaissance

Cette phase consiste à rassembler des renseignements vis à vis la cible.

- Whois, DNS, Scann pour mapper un réseau cible et avoir une idée à propos des systèmes d'exploitation utilisés et les applications déployées
- Tester les périphériques de filtrage
- Chercher du trafic confidentiel
- Vérifier l'installation par default (login et mots de passe ...)

Cette phase de reconnaissance peut être classée sous deux formes:

- Passive: Chercher l'information publiée par la cible
- Active: Entrer en interaction avec la cible

Les phases du PenTest

Le scann

- C'est la pré-attaque
- Consiste à mapper le système, les routeurs, les parfeu (Traceroute)
- Scanner les ports pour découvrir les services déployés chez une cible
- Utiliser des scanneurs de vulnérabilités

Les phases du PenTest

Le gain d'accès

- Accéder au système d'exploitation, au réseau ou bien à une application
- Gagner plus de privilèges (escalader les privilèges)
- Cracker les mots de passe, buffer overflows, DoS, Session hijacking

Les phases du PenTest

Maintenance de l'accès

- L'attaquant essaye de se laisser un meilleur accès au système en cas de détection (Backdoor; toolkits, trojan)
- Utiliser le système corrompu pour lancer des attaques (attaque par rebond)

Les phases du PenTest

Effacer les traces

Effacer les traces des tests et rendre un rapport des vulnérabilités trouvées.

Outils de PenTest

Un tas d'outils (libres même) sont présents sur Internet qu'on peut utiliser pour les test de pénétration:

- Nessus (openvas): un scanner de vulnérabilités
- Metasploit: il permet de développer et de tester des codes d'exploitation
- ...

Plan

Présentation du Footprinting

Présentation

Le Footprinting est l'art de rassemblement d'information à propos d'une cible.

Caractéristiques

- C'est une technique passive
- L'objectif est de rassembler l'information publique à propos de la cible pour lui rassembler un profil correspondant
- Ces informations:
  - Les domaines de la cible et ses sites Web
  - Des informations à propos d'organisations qui sont liées à la cible
  - Les directeurs en charge
  - Les numéros de téléphones, adresses physiques et emails
  - Les événements actuels et archivés
  - Technologies utilisées
  - Les adresses IP publiques
  - ...

Techniques de Footprinting

Internet Footprinting

- *Google hacking*: création de requêtes complexes et précises sur le moteur de recherche Google. Cela est faisable grâce aux opérateurs. Exemples:
  - inurl: admin filetype:xls
  - allintitle: index of (pdf—xls) financial
  - allinurl: admin userlist
  - site: fsr.ac.ma filetype: pdf
  - intitle: Remote.Desktop.Web.Connection inurl: tsweb
  - `https://sites.google.com/site/gwebsearcheducation/advanced-operators`

Techniques de Footprinting

Internet Footprinting

- *archive.org*: ce site web garde plusieurs copies de plusieurs sites web. Cela est très pratique au cas où on essaye d'étudier l'évolution de la cible.
  - pourquoi une telle page a été supprimé? est-ce pour des raisons de sécurité?
  - Pourquoi la liste des salariés changent sans cesse? est-ce que l'entreprise a des problèmes de gestion?
  - que sont les noms des anciens employés? est-ce qu'ils étaient virés?
  - pourquoi une partie du site web a disparu? le projet qu'elle définissait a fini ou bien est abandonné?

Techniques de Footprinting

Internet Footprinting

- *autres sources*:
  - les sites d'emploi et les CV d'employés
  - les forums de discussion
  - les réseaux sociaux
  - l'extraction de méta-données
  - Whois (adresses de serveurs DNS, emails des admin, location physique ...)
  - ingénierie sociale

Outils de Footprinting et contre-mesure

Outils

- The harvester : un script python qui permet d'analyser les serveurs Google, MSN, linkedin pour extraire des adresses emails
- Metagoofil : extrait des informations publiques en analysant les méta-données et les techniques de Google hacking
- Dnsenum : permet d'envoyer des requêtes aux serveurs DNS pour en tirer des informations intéressantes

Contre-mesures

- sensibilisation des employés de la copie des codes de configurations sur les forum
- utilisation des adresses email qui ne révèle pas l'identité de son propriétaire
- bien configurer les serveurs DNS

Plan

Introduction

Présentation

Le scanning permet d'avoir une idée exacte de l'emplacement des machines qui sont à l'écoute du trafic réseau et savoir si elles sont à la portée de l'attaquant.

Introduction

Techniques de scan

- Tracerouting : cette technique utilise le champs TTL des paquets pour détecter les noeuds de routage. Elle permet de découvrir et de mapper la route entre la source et la destination
- Firewalking : cette technique permet de mapper les règles de filtrage qui peuvent être appliquées sur les routeurs et les par-feu. Elle utilise des techniques de tracerouting pour calculer le nombre de sauts entre l'attaquant et une technique qui se trouve derrière le périphérique de filtrage.

Introduction

Tracerouting

- traceroute fr.wikipedia.org
- tcptraceroute -n -f 11 fr.wikipedia.org 80

Firewalking

Le résultat de l'envoi de paquet ici peut avoir trois sens:

- Une erreur ICMP TIME_EXCEEDED: le paquet a passé depuis le parfeu et a expiré (port ouvert)
- Pas de réponse reçue: le paquet n'a pas réussi de passer depuis le parfeu, probablement supprimé (port probablement fermé)
- Une erreur ICMP ADMINISTRATIVELY_PROHIBITED: le port est fermé

Le scanning des réseaux

Présentation

Le scanning des réseaux permet de détecter les machines actives du réseau scanné.

Techniques

- ARP ping sweeps
- ICMP ping sweeps
- TCP ping sweeps
- ICMP queries

Le scanning de ports

Présentation

Le scanning de ports consiste à découvrir les services TCP/UDP sur une ou plusieurs machines.

- Le scan vertical: scanner plusieurs ports sur une seule machine
- Le scan horizontal: balayer plusieurs machines sur un seul port

Techniques

- TCP connect()
- SYN stealth
- Xmas scan
- FIN scan
- NULL scan
- ACK scan
- FTP bounce scan ...

Outils de scan

- Arp-scan : un outil en ligne de commande pour la découverte de systèmes. Il réalise plusieurs scanns et tests au niveau 2.
- Fping : un outil en ligne de commande qui permet de réaliser des balayage ICMP
- Hping : un forgeur de paquets
- Nmap : l'outil le plus connut du scan
  - -sP : ping scanning
  - -sT : TCP connect() scan
  - -sS : SYN stealth scan
  - -sN : Null scan
  - -sO: IP protocol scan

Plan

Introduction

Présentation

L'écoute de trafic veut dire l'interception de l'information qui circule dans un réseau. Cette technique est souvent utilisé par les administrateurs réseau pour le monitoring de leur parc informatique. Seulement, cela peut être utilisé pour l'écoute d'un trafic confidentiel.

Types d'écoute

- Écoute passive: sur des réseaux où la machine ignore le trafic qui lui provient mais ne lui est pas destinée (wifi, hub)
- Écoute active: sur un réseau commuté (il laisse des traces sur l'équipement réseau et les machines)

Techniques de sniffing

Sniffing sur un medium partagé

- Hub, point d'accès wifi
- promiscuous mode

MAC flooding

Le MAC flooding consiste à submerger une interface du commutateur par de nombreuses adresses MAC. Selon le commutateur, il se peut qu'il y est une panne ou bien il commence à agir comme un hub.

Techniques de sniffing

DHCP starvation

DHCP starvation est un attaque DoS. l'attaquant vise un serveur DHCP et lui envoie assez de requête DHCP pour épuiser sa plage d'adresses.

Rogue DHCP

Rogue DHCP consiste à introduire au réseau un serveur DHCP non autorisé. Ainsi, la distribution des adresses IP se fera selon les besoins de l'attaquant.

Techniques de sniffing

DNS ID spoofing

Le DNS ID spoofing consiste à répondre à des requêtes DNS avant le vrai serveur DNS

DNS Cache poisoning

Elle nécessite un détournement de flux et envoyer des réponses DNS sans laisser les requêtes parvenir au vrai serveur DNS

Outils de sniffing

TCPdump

TCPdump est un outil de sniffing en ligne de commande. Il est disponible sur linux et windows, et peut être utilisé avec plusieurs options.

- -D : afficher la liste des interfaces réseaux depuis lesquels on peut lancer TCPdump
- -i : pour choisir l'interface réseau à utiliser
- -c : pour indiquer le nombre de paquets à écouter
- -n : afficher des adresses au lieu des adresses IP
- -q : afficher de courtes lignes
- -v : pour le mode verbose
- -w : pour mettre la capture dans un fichier
- -r : pour lire un fichier qui contient une capture

Outils de sniffing

Autres

- Wireshark
- Cain
- Snort
- Smac
- Macchanger
- ...